特 許 協 力 条 約

PCT

REC'D 09 JUN 2005
WIPO PCT

特許性に関する国際予備報告（特許協力条約第二章）

（法第12条、法施行規則第56条）
〔ＰＣＴ36条及びＰＣＴ規則70〕

出願人又は代理人の書類記号 ES190401	今後の手続きについては、様式ＰＣＴ／ＩＰＥＡ／４１６を参照すること。	
国際出願番号 ＰＣＴ／ＪＰ２００４／００３５２０	国際出願日 （日．月．年） １７．０３．２００４	優先日 （日．月．年） １７．０３．２００３
国際特許分類（ＩＰＣ） Int.Cl.[7] Ｇ０６Ｆ１／００，Ｇ０６Ｆ１５／００		
出願人（氏名又は名称） セイコーエプソン株式会社		

1．この報告書は、ＰＣＴ35条に基づきこの国際予備審査機関で作成された国際予備審査報告である。
法施行規則第57条（ＰＣＴ36条）の規定に従い送付する。

2．この国際予備審査報告は、この表紙を含めて全部で 4 ページからなる。

3．この報告には次の附属物件も添付されている。

a．☑ 附属書類は全部で 6 ページである。

☑ 補正されて、この報告の基礎とされた及び／又はこの国際予備審査機関が認めた訂正を含む明細書、請求の範囲及び／又は図面の用紙（ＰＣＴ規則70.16及び実施細則第607号参照）

☐ 第Ⅰ欄４．及び補充欄に示したように、出願時における国際出願の開示の範囲を超えた補正を含むものとこの国際予備審査機関が認定した差替え用紙

b．☐ 電子媒体は全部で ＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿ （電子媒体の種類、数を示す）。
配列表に関する補充欄に示すように、コンピュータ読み取り可能な形式による配列表又は配列表に関連するテーブルを含む。（実施細則第802号参照）

4．この国際予備審査報告は、次の内容を含む。

☑ 第Ⅰ欄 国際予備審査報告の基礎
☐ 第Ⅱ欄 優先権
☐ 第Ⅲ欄 新規性、進歩性又は産業上の利用可能性についての国際予備審査報告の不作成
☑ 第Ⅳ欄 発明の単一性の欠如
☑ 第Ⅴ欄 ＰＣＴ35条(2)に規定する新規性、進歩性又は産業上の利用可能性についての見解、それを裏付けるための文献及び説明
☐ 第Ⅵ欄 ある種の引用文献
☐ 第Ⅶ欄 国際出願の不備
☐ 第Ⅷ欄 国際出願に対する意見

国際予備審査の請求書を受理した日 １２．０７．２００４	国際予備審査報告を作成した日 ２５．０５．２００５	
名称及びあて先 日本国特許庁（ＩＰＥＡ／ＪＰ） 郵便番号１００－８９１５ 東京都千代田区霞が関三丁目４番３号	特許庁審査官（権限のある職員） 宮司 卓佳	５Ｓ ９５５５
	電話番号 ０３－３５８１－１１０１ 内線 ３５４６	

様式ＰＣＴ／ＩＰＥＡ／４０９（表紙）（２００４年１月）

特許性に関する国際予備報告

国際出願番号 PCT／JP2004／003520

第Ⅰ欄 報告の基礎

1．この国際予備審査報告は、下記に示す場合を除くほか、国際出願の言語を基礎とした。

☐ この報告は、＿＿＿＿＿＿ 語による翻訳文を基礎とした。
それは、次の目的で提出された翻訳文の言語である。
☐ PCT規則12.3及び23.1(b)にいう国際調査
☐ PCT規則12.4にいう国際公開
☐ PCT規則55.2又は55.3にいう国際予備審査

2．この報告は下記の出願書類を基礎とした。（法第6条（PCT14条）の規定に基づく命令に応答するために提出された差替え用紙は、この報告において「出願時」とし、この報告に添付していない。）

☐ 出願時の国際出願書類

☑ 明細書
第 1－17 ページ、出願時に提出されたもの
第＿＿＿＿ ページ*、＿＿＿＿ 付けで国際予備審査機関が受理したもの
第＿＿＿＿ ページ*、＿＿＿＿ 付けで国際予備審査機関が受理したもの

☑ 請求の範囲
第 3-5, 8, 10, 12, 13, 17 項、出願時に提出されたもの
第＿＿＿＿ 項*、PCT19条の規定に基づき補正されたもの
第 1, 2, 6, 7, 9, 11, 15, 16, 18, 20, 21 項*、14．01．2005 付けで国際予備審査機関が受理したもの
第＿＿＿＿ 項*、＿＿＿＿ 付けで国際予備審査機関が受理したもの

☑ 図面
第 1－6 図、出願時に提出されたもの
第＿＿＿＿ ページ／図*、＿＿＿＿ 付けで国際予備審査機関が受理したもの
第＿＿＿＿ ページ／図*、＿＿＿＿ 付けで国際予備審査機関が受理したもの

☐ 配列表又は関連するテーブル
配列表に関する補充欄を参照すること。

3．☑ 補正により、下記の書類が削除された。
☐ 明細書 第＿＿＿＿ ページ
☑ 請求の範囲 第 14，19 項
☐ 図面 第＿＿＿＿ ページ／図
☐ 配列表（具体的に記載すること）＿＿＿＿
☐ 配列表に関連するテーブル（具体的に記載すること）＿＿＿＿

4．☐ この報告は、補充欄に示したように、この報告に添付されかつ以下に示した補正が出願時における開示の範囲を超えてされたものと認められるので、その補正がされなかったものとして作成した。（PCT規則70.2(c)）
☐ 明細書 第＿＿＿＿ ページ
☐ 請求の範囲 第＿＿＿＿ 項
☐ 図面 第＿＿＿＿ ページ／図
☐ 配列表（具体的に記載すること）＿＿＿＿
☐ 配列表に関連するテーブル（具体的に記載すること）＿＿＿＿

＊ 4．に該当する場合、その用紙に "superseded" と記入されることがある。

特許性に関する国際予備報告

国際出願番号 PCT／JP2004／003520

第Ⅳ欄　発明の単一性の欠如

1．　請求の範囲の減縮又は追加手数料の納付の求めに対して、出願人は、

☐ 請求の範囲を減縮した。

☐ 追加手数料を納付した。

☐ 追加手数料の納付と共に異議を申立てた。

☑ 請求の範囲の減縮も、追加手数料の納付もしなかった。

2．☐ 国際予備審査機関は、次の理由により発明の単一性の要件を満たしていないと判断したが、ＰＣＴ規則68.1の規定に従い、請求の範囲の減縮及び追加手数料の納付を出願人に求めないこととした。

3．　国際予備審査機関は、ＰＣＴ規則 13.1、13.2 及び 13.3 に規定する発明の単一性を次のように判断する。

☐ 満足する。

☑ 以下の理由により満足しない。

請求の範囲１－２１に係る発明に共通する事項は、独立項である請求の範囲１，６，１７，１８，２０及び２１の記載からすると、ウィルスが侵入したとき通信情報を取得し、取得した通信情報の基づいて、ウィルスの送信元となっているコンピュータを検出することのみである。
しかしながら、調査の結果、当該共通事項は以下の文献に記載されているように新規でないことが明らかになった。

文献：JP 11-134190 A(株式会社日立製作所) 1999.05.21, 全文,第１－５図
(ファミリーなし)

つまり、当該文献には、ネットワーク上を転送されるデータに対してウィルスチェックを行い、ウィルス感染が検出されると、ウィルスが添付された電子メール又は文書ファイルを送信したコンピュータを送信された情報に基づいて検出することが記載されている。
結果として、上記共通事項は先行技術の域を出ないから、上記共通事項をもって請求の範囲１－２１に係る発明が、単一の一般的発明概念を形成するように関連しているとは認められない。
そして、請求の範囲１－１３，１５－１８及び２０に係る発明に共通する事項は、ウィルスの送信元コンピュータに対してウィルス攻撃処理を行うことであるのに対して、請求の範囲２１に係る発明は、ウィルス攻撃処理を行うものでないから、請求の範囲１－１３，１５－１８及び２０に係る発明と、請求の範囲２１に係る発明とは、単一の一般的発明概念を形成するように関連しているとは認められない。
したがって、請求の範囲１－１３，１５－１８及び２０に係る発明と、請求の範囲２１に係る発明とは、発明の単一性の要件を満たしていない。

4．　したがって、国際出願の次の部分について、この報告を作成した。

☐ すべての部分

☑ 請求の範囲 １－１３，１５－１８及び２０ に関する部分

特許性に関する国際予備報告

国際出願番号 ＰＣＴ／ＪＰ２００４／００３５２０

第Ⅴ欄　新規性、進歩性又は産業上の利用可能性についての法第12条（ＰＣＴ35条(2)）に定める見解、それを裏付ける文献及び説明

1．　見解

新規性（N）	請求の範囲	１－１３，１５－１８，２０	有
	請求の範囲		無
進歩性（ＩＳ）	請求の範囲	１－１３，１５，１６，１８，２０	有
	請求の範囲	１７	無
産業上の利用可能性（ＩＡ）	請求の範囲	１－１３，１５－１８，２０	有
	請求の範囲		無

2．　文献及び説明（ＰＣＴ規則70.7）

文献１：JP 2002-252654 A(三菱電機株式会社) 2002.09.06
文献２：WO 2002/006928 A(VCIS INC.) 2002.06.14
文献３：なぜこんな製品がないのだろう，コンピュータ＆ネットワークＬＡＮ，第１７巻，第１２号，(日)，株式会社オーム社，1999.12.01，第４５－第４７頁
文献４：JP 2002-73433 A(三菱電機株式会社) 2002.03.12
文献５：JP 2003-36243 A(ケイディーディーアイ株式会社) 2003.02.07
文献６：JP 11-134190 A(株式会社日立製作所) 1999.05.21，全文，全図
(ファミリーなし)

請求の範囲１７は、国際調査報告で引用された文献１により進歩性を有しない。
文献１には、コンピュータネットワークにおいて、エージェントをリモート操作することにより、複数の送信元から攻撃対象の送信先へ一斉にパケットを送信するＤＤｏＳ攻撃、及び不正アクセスの侵入が検出された場合に、パケット中継を自動的に禁止する構成が記載されており、攻撃の手段として、文献１のパケットを一斉に送信先に送信する構成を採用することは当業者にとっては自明のものである。

請求の範囲１－１３，１５，１６，１８及び２０は、国際調査報告で引用された文献１乃至５及び新たに引用する文献６に対し新規性・進歩性を有する。
上記文献には、ウィルス攻撃処理を行う又は攻撃開始を予告するメッセージを送信すること、及び、攻撃開始時もしくは攻撃開始以後、攻撃元の端末装置で警報音を発生することは、上記文献のいずれにも記載されておらず、また、上記文献の記載から当業者が容易に想到し得たものともいえない。

請求の範囲

1．（補正後） ネットワークでのウィルスの感染を検出して、ウィルスの感染を阻止する方法であって、

ウィルスが侵入したとき通信情報を取得し、取得した通信情報に基づいて、ウィルスの送信元となっているコンピュータを検出し、ウィルスの送信元となっているコンピュータに対して、ネットワークを介してウィルスの活動を抑制するウィルス攻撃処理を行うことを予告するメッセージを送信し、当該ウィルスの送信元となっているコンピュータに対して、ウィルス攻撃処理を行うことを特徴とするウィルスの感染を阻止する方法。

2．（補正後） 請求項1に記載のウィルスの感染を阻止する方法において、

ネットワークを介してアクセス可能なおとりを、ウィルスの侵入を監視するコンピュータ上に設けて、ネットワークを介して前記おとりに対するアクセスを受け付けて、通信情報を取得すると共に、ウィルスの侵入を検出し、

前記おとりは、おとりフォルダを記憶装置に記憶させたもの、おとりアプリケーションを記憶装置に記憶させたもの、および、記憶装置に擬似的に形成したサーバ、のうち1以上であるウィルスの感染を阻止する方法。

3． 請求項1に記載のウィルスの感染を阻止する方法において、

前記ウィルス攻撃は、前記ウィルスの送信元となっているコンピュータに高負荷を与えるものであるウィルスの感染を阻止する方法。

4． 請求項3に記載のウィルスの感染を阻止する方法において、

前記ウィルスの送信元となっているコンピュータに与える高負荷は、

当該コンピュータのトラフィックを増大させることであるウィルスの感染を阻止する方法。

5． 請求項3に記載のウィルスの感染を阻止する方法において、
前記ウィルスの送信元となっているコンピュータに与える高負荷は、当該コンピュータのＣＰＵが応答動作をすべき処理を大量に要求することであるウィルスの感染を阻止する方法。

6．（補正後） ネットワークでのウィルスの感染を検出して、ウィルスの感染を阻止するシステムであって、
ウィルスの侵入を検出し、かつ、ウィルスの侵入を検出した時、ウィルスの侵入時に取得した通信情報から当該ウィルスの送信元となっているコンピュータを検出する通信情報解析手段と、
ウィルスの送信元となっているコンピュータに対して、ネットワークを介してウィルスの活動を抑制するウィルス攻撃処理を行うコンピュータ攻撃手段と、
感染したコンピュータに対して、攻撃開始を予告するためのメッセージを送信する手段と、
を備えることを特徴とするウィルスの感染を阻止するシステム。

7．（補正後） 請求項6に記載のウィルスの感染を阻止するシステムにおいて、
ネットワークを介してアクセスが可能なおとり手段をさらに備え、
前記通信情報解析手段は、前記おとり手段へのウィルスの侵入を検出し、かつ、ウィルスの侵入を検出した時、ウィルスの侵入時に取得した通信情報から当該ウィルスの送信元となっているコンピュータを検出するものであるウィルスの感染を阻止するシステム。

8． 請求項6に記載のウィルスの感染を阻止するシステムにおいて、

前記コンピュータ攻撃手段は、前記ウィルスの送信元となっているコンピュータに高負荷を与えるものであるウィルスの感染を阻止するシステム。

9．（補正後）　請求項8に記載のウィルスの感染を阻止するシステムにおいて、
前記コンピュータ攻撃手段は、前記ウィルスの送信元となっているコンピュータのトラフィックを増大させて、当該コンピュータ高負荷を与えることであるウィルスの感染を阻止するシステム。

10．　請求項8に記載のウィルスの感染を阻止するシステムにおいて、
前記コンピュータ攻撃手段は、前記ウィルスの送信元となっているコンピュータのＣＰＵが応答動作をすべき処理を大量に要求して、当該コンピュータに高負荷を与えることであるウィルスの感染を阻止するシステム。

11．（補正後）　請求項6、7、8、9および10のいずれか一項に記載のウィルスの感染を阻止するシステムにおいて、
ウィルスの送信元となっているコンピュータの管理者宛の検出報告を発する手段をさらに備え、
前記コンピュータ攻撃手段は、当該ウィルスへの対策が完了するまで、当該コンピュータへの攻撃を継続するウィルスの感染を阻止するシステム。

12．　請求項6に記載のウィルスの感染を阻止するシステムにおいて、
前記おとり手段は、ネットワークに接続されたコンピュータの記憶装置上に擬似的に形成した、おとりサーバ中に設けられたアプリケーショ

ンにより構成されるおとりフォルダであるウィルスの感染を阻止するシステム。

１３．　請求項６に記載のウィルスの感染を阻止するシステムにおいて、

前記おとり手段は、ネットワークに接続されたコンピュータの記憶装置上に擬似的に形成した、おとりサーバ中に設けられたアプリケーションにより構成されるおとりアプリケーションであるウィルスの感染を阻止するシステム。

１４．（削除）

１５．（補正後）　請求項６、７、８、９および１０のいずれか一項に記載のウィルスの感染を阻止するシステムにおいて、

攻撃開始時もしくは攻撃開始以後、攻撃元の端末装置で警報音を発生する手段をさらに備えるウィルスの感染を阻止するシステム。

１６．（補正後）　請求項６、７、８、９および１０のいずれか一項に記載のウィルスの感染を阻止するシステムにおいて、

ネットワークに接続された別のコンピュータに対して、ウィルス送信元となっているコンピュータのネットワークアドレスを通知するとともに、ウィルスの送信元となっているコンピュータに対してウィルス攻撃処理を行うことを依頼する手段をさらに備えるウィルスの感染を阻止するシステム。

１７．　ネットワークでのウィルスの感染を検出して、ウィルスの感染を阻止するシステムであって、

ウィルスの送信元となっているコンピュータに対してウィルス攻撃処理を行うことについての依頼を受ける手段と、

前記受けた依頼に基づいて、前記ウィルスの送信元となっているコンピュータに対して、ネットワークを介してウィルスの活動を抑制するウィルス攻撃処理を行うコンピュータ攻撃手段と、を備えることを特徴とするウィルスの感染を阻止するシステム。

１８．（補正後） ウィルスの侵入を検出し、かつ、ウィルスの侵入を検出した時、ウィルスの侵入時に取得した通信情報から当該ウィルスの送信元となっているコンピュータを検出する通信情報解析手段と、

ウィルスの送信元コンピュータに対して、ネットワークを介してウィルスの活動を抑制するウィルス攻撃処理を行うコンピュータ攻撃手段と、

感染したコンピュータに対して、攻撃開始を予告するためのメッセージを送信する手段と、をコンピュータに構築させる、ウィルスの感染を阻止するプログラム。

１９．（削除）

２０．（追加） ネットワークでのウィルスの感染を検出して、ウィルスの感染を阻止するシステムであって、

ウィルスの侵入を検出し、かつ、ウィルスの侵入を検出した時、ウィルスの侵入時に取得した通信情報から当該ウィルスの送信元となっているコンピュータを検出する通信情報解析手段と、

ウィルスの送信元となっているコンピュータに対して、ネットワークを介してウィルスの活動を抑制するウィルス攻撃処理を行うコンピュータ攻撃手段と、

攻撃開始時もしくは攻撃開始以後、攻撃元の端末装置で警報音を発生する手段と、

を備えることを特徴とするウィルスの感染を阻止するシステム。

21．（追加） ネットワークでのウィルスの感染を検出して、ウィルスの感染を阻止するシステムであって、

ウィルスの侵入を検出し、かつ、ウィルスの侵入を検出した時、ウィルスの侵入時に取得した通信情報から当該ウィルスの送信元となっているコンピュータを検出する通信情報解析手段と、

ウィルスの送信元となっているコンピュータの管理者宛の検出報告を発する手段と、を備えることを特徴とするウィルスの感染を阻止するシステム。